ABSTRACT OF THE DISCLOSURE

METHOD AND SYSTEM FOR NETWORK SINGLE SIGN-ON USING A PUBLIC KEY CERTIFICATE AND AN ASSOCIATED ATTRIBUTE CERTIFICATE

A methodology is presented for a network single sign-on (SSO) authentication process using digital certificates. A user has access to protected resources, such as legacy applications, that require verification of a user's authentication data prior to providing access. The user's authentication data is encrypted using the public key of the user, and an attribute certificate containing the encrypted authentication data is generated by an attribute-certificate-issuing authority. When a user requires access to the protected resource, an SSO agent performs an initial authentication process against the user. The SSO agent then retrieves the user's attribute certificate, and for subsequent authentication requests for other protected resources, the SSO agent uses the authentication data from the attribute certificate that corresponds to the targeted protected resource. The SSO agent forwards the required authentication data to the protected resource, and the protected resource then authenticates a user based on the provided authentication data.